UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,432	06/25/2003	Terence Spies	ID-8	6320

36532 7590 01/12/2007

G. VICTOR TREYZ
FLOOD BUILDING
870 MARKET STREET, SUITE 984
SAN FRANCISCO, CA 94102

EXAMINER	
SANDOVAL, KRISTIN D	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/606,432	SPIES ET AL.	
	Examiner	Art Unit	
	Kristin D. Sandoval	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-28* is/are rejected.

7)☒ Claim(s) *3* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/8/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-4, 6-10, 12-14, 18, 21 and 24-26 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

With regard to claims 1-4 and 6-9 it is unclear what the scope of the claims entail since claim 2 does not seem to further limit independent claim 1 unless using a key to encrypt something is not encrypting something with a key. Otherwise, claims 3, 4 and 6-9 conflict with the independent claim. If using a public key to encrypt a public key implies that the public key was encrypted with the other public key in a public key/private key algorithm, then claim 3 conflicts with claim 1 since now the same two keys are not encrypting each other, a symmetric key is being used to encrypt a public key and then a public key is being used to encrypt the symmetric key. If this is the case then claim 4 contradicts claim 3 since you don't need the symmetric key in order to decrypt the public key in encrypted. And if in independent claim 1, the message is encrypted using a public key then encrypting the same message in claim 6 contradicts claim 1.

The terms "more-sensitive and less-sensitive" in claims 10, 13, 19 and 21 is a relative term which renders the claim indefinite. The terms "more-sensitive and less-sensitive" are not

defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim 18 recites the limitation "the inner layer of the message" in lines 4-5. There is insufficient antecedent basis for this limitation in the claim.

With regard to claims 24-26, again it is unclear whether, since the public key QG is already encrypted with symmetric key S in claim 21, it seems that claim 24 conflicts with claim 21. It is unclear whether public key QG is encrypted with S' before or after S or if it is another embodiment entirely. If it is another embodiment entirely then it would appear that it is the same as encrypting public key QG with S just with S' and since S and S' could be equal it is unclear.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, 4, 5, 6-9, 13, 16, 18, 21-23, 24-28 rejected under 35 U.S.C. 103(a) as being unpatentable over Slick et al. (Slick), U.S. Patent No. 7,003,667 in view of Boneh et al. (Boneh), U.S. Patent No. 7,113,594.

As per claims 1 and 2:

Slick substantially teaches a method comprising:

at the sender, encrypting the message using at least two layers of encryption by using an inner layer of message encryption having an associated inner-layer public key to encrypt the message data and by using an outer layer of message encryption having an associated outer-layer public key to encrypt the inner-layer public key without using a symmetric key; sending the encrypted message to the recipient; and at the recipient, decrypting the encrypted message using an outer-layer private key corresponding to the outer-layer public key and using an inner-layer private key corresponding to the inner layer public key (9:27-10:45, 11:20-28, 11:42-64 wherein it would have been obvious to combine the one embodiment of Slick that uses a public key to encrypt the public key that encrypts the symmetric key with the embodiment that encrypts the message using the public key and then encrypting the public key encrypted message again utilizing the first embodiment as suggested by Slick (11:64-67). Since encrypting the message twice with a public key utilizes a lot of system resources, encrypting only the key saves resources while ensuring security (11:67-12:7).

As per claim 4:

Slick substantially teaches a method further comprising:

sending the encrypted message to the recipient comprises sending the encrypted inner-layer public key to the recipient with the encrypted message, and wherein decrypting the encrypted message at the recipient further comprises using the outer-layer private key to decrypt the encrypted inner-layer public key to produce an unencrypted version of the inner-layer public key at the recipient (1:39-58).

As per claim 5:

Slick further teaches a method wherein encrypting the message comprises encrypting the message using at least three layers of encryption and wherein the outer layer is not an outermost layer (10:46-11:28 wherein three keys equals three layers but the third is not the outermost layer since a signed hash can also be appended).

As per claims 6-8, 21-23 and 24-26:

Slick teaches a method comprising:

encrypting the message by performing at least an inner layer of encryption and an outer layer of encryption at the sender, wherein: performing the inner layer of encryption includes encrypting the message data M using a symmetric key S to produce encrypted message data Ms and encrypting the symmetric key S using an public key QG associated with the inner layer of encryption to produce an encrypted symmetric message key SQG, and performing the outer layer of encryption includes encrypting at least the public key QG using an public key QL, wherein the public key QL is less sensitive than the public key QG; and sending at least the encrypted message data Ms, the encrypted symmetric message key SQG, the public key QL, the encrypted key QGQL and the encrypted public key QG to the recipient (9:27-10:45, 11:4-28).

As per claim 9:

Slick teaches a method further comprising:

using the outer-layer private key to decrypt the inner-layer public key that has been encrypted using the outer-layer public key; using inner-layer private key to decrypt the symmetric key that has been encrypted using the inner-layer public key; and using the symmetric key that has been decrypted using the inner-layer private key to decrypt the message data that was encrypted using the symmetric key (12:7-51).

As per claim 13:

Slick further teaches a method wherein at least one of the data attributes has an associated sensitivity level and wherein encrypting the message data comprises using the sensitivity level in determining how to encrypt the message (1:14-22).

As per claims 15 and 16:

Boneh further teaches a method wherein encrypting an email message comprises utilizing an age based policy (29:55-63).

As per claims 27 and 28:

Boneh further teaches a public key based on a recipient's email address (2:45-62).

Slick fails to disclose the key and encryption being IBE, however, Boneh discloses utilizing IBE as an asymmetric encryption scheme (abstract). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to make the keys be identity based as suggested by Slick, in order to ensure the intended recipients receive the printout or fax, having keys based on their identity would ensure that only they could read it and only printers or fax machines associated with them could decrypt the information (Slick, 1:14-58).

4. Claims 10, 11 and 18-20 rejected under 35 U.S.C. 103(a) as being unpatentable over Slick in view of Boneh as applied to claim 1 above, and further in view of Van Oorschot et al. (Van Oorschot), U.S. Patent No. 5,850,443.

As per claims 10 and 18-20:

Slick and Boneh fail to disclose varying sensitivity levels of the multiple encryption keys and the keys having overlapping components. However, Van Oorschot discloses a method

wherein varying strengths of multiple encryption keys are used and the keys are concatenated together, therefore each key shares the same components with all the others (4:16-56).

It would have been obvious to utilize varying encryption key strengths along with overlapping components because it allows multiple parties to communicate over varying trust environments and to share cryptographic keys (Van Oorschot, 1:66-2:13).

As per claim 11:

Slick further teaches a method wherein encrypting the message comprises encrypting the message using at least three layers of encryption and wherein the outer layer is not an outermost layer (10:46-11:28 wherein three keys equals three layers but the third is not the outermost layer since a signed hash can also be appended).

5. Claim 17 rejected under 35 U.S.C. 103(a) as being unpatentable over Slick in view of Boneh as applied to claim 1 above, and further in view of Lord et al. (Lord), U.S. Patent No. 7,131,003.

With regard to claim 17, Slick and Boneh fail to teach the encrypted message comprising an instant message. However, Lord discloses a method of encrypting instant messages (2:35-49). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to increase the security of instant messages as suggested by Lord (1:41-62).

Allowable Subject Matter

6. Claim 3 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin D. Sandoval whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Kristin D Sandoval
Examiner
Art Unit 2132

KDS
KDS

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100